June 2014
Volume 9, Issue 6

Bots, Botnets, and Zombies

Enterprise Security and Risk Management Office

Monthly Security Tips
NEWSLETTER

From the Desk of Chip Moore

What are Bots, Botnets and Zombies?

You have probably heard terms such as "bots," "zombies," and "botnets" in recent news stories about data breaches and other cyber security risks. But what exactly are they, how do they work, and what damage can they cause?

A "bot," short for "robot," is a type of software application or script that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer. The compromised machine may be referred to as a "zombie." A collection of these infected computers is known as a "botnet."

Hundreds of millions of computers worldwide are infected with bots and under the control of hackers (i.e., part of a botnet). The owners of these computers typically do not experience any signs that the machine is infected and continue to use it, unaware they are being controlled remotely by a cyber criminal. In fact, the infected machine could be sending multiple spam emails, including to all contacts in the computer, making it appear to the recipient that the email is legitimate and from someone they know.

A botnet that has recently been in the news is the Gameover Zeus Botnet, which allows cyber criminals to retrieve banking passwords from the infected machines, or use the botnet to infect more computers. This botnet was responsible for nearly one million infections worldwide since its first attack in September 2011.[i] In June 2014, U.S. and international law enforcement seized control of the botnet, and are working with Internet service providers (ISP) to notify impacted victims.

How and Why Do Cyber Criminals Use Botnets?

- The value of bots and botnets to criminals comes from aggregating massive numbers of computers they can control simultaneously to perform malicious activities.
- Cyber criminals may use the botnets to send spam, phishing emails, or other scams to trick consumers into giving up their financial information.
- Cyber criminals may also collect information from the bot-infected machines and use it to steal identities, incurring loans and purchase charges under the user's name.
- Cyber criminals may use botnets to create denial-of-service (DoS) attacks that flood a legitimate service or network with a crushing volume of traffic. The volume may severely slow down, or even shut down, the organization's business operations. Revenue from DoS attacks comes through extortion and leasing botnets. The criminals will rent botnets to groups interested in inflicting damage to another entity. The "renters" will use the botnet for sending spam and phishing emails or attacking legitimate websites and networks. These groups include "hacktivists" — hackers with political agendas—as well as foreign military and intelligence organizations.

Don’t Let Your Computer Become a Bot

It only takes moments for an unprotected, Internet-connected computer to be infected with malicious software and be turned into a bot. Every user should have up-to-date security software on all their devices.

The best protection is to set your anti-virus and anti-spyware programs to automatically update, and to automatically install every patch made available for your operating system and browser.

Do not click on links in unsolicited emails.

Do not click on links from your friends and family if *they* are not using updated security measures. They may unknowingly transmit an infection on their machine to yours.

While there is no single action that will protect you from all of the cyber risks, by implementing these foundational best practices, you can greatly reduce the likelihood that your computer will be caught in the next botnet.

Sources and References

[1] http://www.usatoday.com/story/news/nation/2014/06/02/global-cyber-fraud/9863977/

Microsoft: What Is a Botnet
http://www.microsoft.com/security/resources/botnet-whatis.aspx

CIS and NCSA: Botnet Fact Sheet
http://staysafeonline.org/ncsam/resources/botnet-fact-sheet

Provided By:

CENTER FOR INTERNET SECURITY | STOP | THINK | CONNECT